Lesley E. Weaver (SBN 191305)
BLEICHMAR FONTI & AULD LLP
555 12th Street, Suite 1600
Oakland, CA 94607
Tel.: (415) 445-4003
Fax: (415) 445-4020
lweaver@bfalaw.com

Derek W. Loeser (admitted *pro hac vice)*
KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3200
Seattle, WA 98101
Tel.: (206) 623-1900
Fax: (206) 623-3384
dloeser@kellerrohrback.com

Plaintiffs' Counsel
[*Additional counsel listed on signature page*]

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

STEVEN AKINS, SAMUEL ARMSTRONG, TERRY FISCHER, TAUNNA JARVIMAKI, TYLER KING, GRETCHEN MAXWELL, KIMBERLY ROBERTSON, CHERYL SENKO, TONYA SMITH, and CHARNAE TUTT, on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

FACEBOOK, INC., a Delaware corporation,

Defendant.

Case No.

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiffs, individually and as representatives of a class of similarly situated persons, by their undersigned counsel, allege as follows:

NATURE OF THE CASE

1. This class action concerns a grievous and unprecedented breach of trust and invasion of privacy by which Defendant Facebook, Inc. ("Facebook") allowed third parties such as Cambridge Analytica, LLC ("Cambridge Analytica") and other unknown third parties access to, and the potential unlimited use of, vast amounts of sensitive personal information, including names, birthdates, locations, photos, videos, and likes ("Personal Information")[1] from Facebook users without their consent.

2. Facebook operates a social networking platform where its users provide their Personal Information to Facebook under the belief and agreement that Facebook will safeguard that information, and that Facebook will share the information only with the persons, entities, and groups with whom the user consents. Instead of safeguarding this sensitive Personal Information, Facebook provided it to third party application ("app") developers and other business partners without user consent. Once the user data was in the possession of the third parties, Facebook exercised no control over how those third parties used the data.

3. Cambridge Analytica, through the use of one such third party app developer, obtained Personal Information from more than 87 million Facebook users which it thereafter used to create targeted political advertising and messaging in various United States elections. Moreover, this intentional massive data exfiltration is not an isolated incident but simply a high-profile exemplar.

4. While the Cambridge Analytica incident has made the headlines only in recent months, Facebook has been aware of concerns raised by privacy experts, regulators and users

[1] Personal Information" refers to information that can be used to distinguish or trace an individual's identity, such as name, address, race, gender, orientation, education, compensation, date and place of birth, mother's maiden name, and biometric records, as well as information linked to that individual, including activities such as likes, shares, associations, relationships and status, as well as political, religious, financial data or emotions.

regarding third party access, aggregation, distribution, and use of its users' sensitive Personal Information since at least 2010.

5. In 2011, the Federal Trade Commission ("FTC") finalized a formal complaint, alleging that Facebook's policies and practices threatened user privacy. Specifically, the complaint stated that Facebook's policies regarding third party developers were misleading and deceptive.[2] Facebook entered into a settlement with the FTC where Facebook is: 1) barred from making misrepresentations about the privacy or security of consumers' personal information; and 2) required to obtain consumers' affirmative express consent before enacting changes that override their privacy preferences.[3] In response to this settlement, Mark Zuckerberg, founder and Chief Executive Officer of Facebook, made the following statement:

> [T]his means we're making a clear and formal long-term commitment to do the things we've always tried to do and planned to keep doing -- giving you tools to control who can see your information and then making sure only those people you intend can see it.[4]

6. Facebook assures users that they own and control all the information they post on Facebook—a false and misleading statement. Facebook continues to induce its users into giving up information through its false promises of privacy while surreptitiously providing that information to third parties to generate revenue and while failing to take appropriate steps to safeguard Facebook users' Personal Information from unauthorized access, aggregation, distribution, and use.

---

[2]https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookcmpt.pdf. The FTC complaint outlined the Commission's findings that Facebook made promises it did not keep when: 1) Facebook represented that third party apps its users installed would only have access to the user information needed to operate, when in fact, the apps could access nearly all of a user's personal data - data the apps didn't need; and 2) Facebook told users they could restrict sharing of data to limited audiences - for example with "Friends Only," when in fact, selecting "Friends Only" did not prevent their information from being shared with third party applications their friends used. *Id*.

[3] https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep.

[4] https://www.cnbc.com/2018/03/21/facebook-ceo-mark-zuckerbergs-statements-on-privacy-2003-2018.html.

7. Only after public outcry has Facebook proposed remedial measures. Yet, these proposed measures remain feeble and hollow. None of these stopgap measures adequately remedy or prevent the improper and illegal conduct alleged. In fact, users' data remains dangerously unprotected and open to further abuse by third parties and anyone to whom these third party app developers distribute the users' data.

8. Facebook's disregard for the protection of Plaintiffs' and class members' Personal Information has led Plaintiffs to bring this suit to protect their privacy interests and those of the class.

JURISDICTION, VENUE, AND CHOICE OF LAW

9. Pursuant to 28 U.S.C. § 1331, this Court has original subject matter jurisdiction over the claims that arise under the Stored Communications Act, 18 U.S.C. §§ 2701, *et. seq*. This Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

10. In addition to federal question jurisdiction, this Court also has diversity jurisdiction pursuant to 28 U.S.C. § 1332(d) under the Class Action Fairness Act ("CAFA"), because the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and at least one class member is a citizen of a state different from Facebook.

11. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because Facebook does business in and is subject to personal jurisdiction in this District. Venue is also proper because a substantial part of the events or omissions giving rise to the claim occurred in, or emanated from this District.

12. Facebook's Terms of Service, ¶ 15.1, provide in relevant part:

> You will resolve any claim, cause of action or dispute (claim) you have with us arising out of or relating to this Statement or Facebook exclusively in the U.S. District Court for the Northern District of California or a state court located in San Mateo County, and you agree to submit to the personal jurisdiction of such courts for the purpose of litigating all such claims. The laws of the State of California will

govern this Statement, as well as any claim that might arise between you and us, without regard to conflict of law provisions.[5]

13. Facebook's choice-of-law and venue provision in its contract with Plaintiffs and the class members provide an additional reason why venue is additionally proper in this District, and establishes that California law applies to Plaintiffs' and all class members' claims.

PARTIES

Plaintiffs

14. Plaintiff Steven Akins is a citizen and resident of the State of Tennessee. Plaintiff maintained a Facebook account during the relevant period. Plaintiff's Personal Information was exposed to third parties without his knowledge or consent.

15. Plaintiff Samuel Armstrong is a citizen and resident of the State of Indiana. Plaintiff maintained a Facebook account during the relevant period. Plaintiff's Personal Information was exposed to third parties without his knowledge or consent.

16. Plaintiff Terry Fischer is a citizen and resident of the State of Washington. Plaintiff maintained a Facebook account during the relevant period. Plaintiff's Personal Information was exposed to third parties without her knowledge or consent.

17. Plaintiff Taunna Jarvimaki is a citizen and resident of the State of Washington. Plaintiff maintained a Facebook account during the relevant period. Plaintiff's Personal Information was exposed to third parties without her knowledge or consent.

18. Plaintiff Tyler King is a citizen and resident of the State of Texas. Plaintiff maintained a Facebook account during the relevant period. Plaintiff's Personal Information was exposed to third parties without her knowledge or consent.

[5] Terms of Service, Statement of Rights and Responsibilities, FACEBOOK, https://www.facebook.com/terms.php.

Case 3:18-md-02843-VC Document 144-2 Filed 09/19/18 Page 6 of 26

19. Plaintiff Gretchen Maxwell is a citizen and resident of the State of Texas. Plaintiff maintained a Facebook account during the relevant period. Plaintiff's Personal Information was exposed to third parties without her knowledge or consent.

20. Plaintiff Kimberly Robertson is a citizen and resident of the State of Illinois. Plaintiff maintained a Facebook account during the relevant period. Plaintiff's Personal Information was exposed to third parties without her knowledge or consent.

21. Plaintiff Cheryl Senko is a citizen and resident of the State of Ohio. Plaintiff maintained a Facebook account during the relevant period. Plaintiff's Personal Information was exposed to third parties without her knowledge or consent.

22. Plaintiff Tonya Smith is a citizen and resident of the State of Alabama. Plaintiff maintained a Facebook account during the relevant period. Plaintiff's Personal Information was exposed to third parties without her knowledge or consent.

23. Plaintiff Charnae Tutt is a citizen and resident of the State of Georgia. Plaintiff maintained a Facebook account during the relevant period. Plaintiff's Personal Information was exposed to third parties without her knowledge or consent.

Defendant

24. Defendant Facebook, Inc. ("Facebook"), a publicly traded company, is incorporated in the State of Delaware, with its headquarters located at 1 Hacker Way, Menlo Park, California 94025. Facebook is an online social media and social networking service company founded in 2004. Facebook operates a social networking website that enables users to connect, share, and communicate with each other through text, photographs, and videos as well as to interact with third party apps such as games and quizzes on mobile devices and personal computers.

FACTUAL BACKGROUND

A. Facebook's Collection of Users' Personal Information and Third Party Access

25. Since its inception in 2004, Facebook has grown to become synonymous with interconnectedness in the age of social media. Facebook now has over two billion monthly active users, with over 200 million in the United States alone.[6] With each user sharing Personal Information in order to access the website, Facebook has become one of the world's largest repositories of personal data.[7]

26. While Facebook may have started as a platform designed to service social connections, Facebook's focus has steadily shifted to data mining. Facebook's business model is now centered around finding ways to harness and sell the ability to influence its users' behavior.

27. In May 2007, Facebook unveiled Facebook Platform, calling on all developers to build the next-generation of applications with deep integration into Facebook, distribution across its "social graph," and an opportunity to build new business.[8] Facebook CEO Mark Zuckerberg told the audience of 750 developers and partners: "Until now, social networks have been closed platforms. Today, we're going to end that. With this evolution of Facebook Platform, any developer worldwide can build full social applications on top of the social graph, inside of Facebook." Zuckerberg continued, "This is good for us because if developers build great applications then they're providing a service to our users and strengthening the social graph, […] This is a big opportunity. We provide the integration and distribution and developers provide the applications. We help users share more information and together we benefit."[9]

---

[6] https://www.statista.com/statistics/398136/us-facebook-user-age-groups/; https://newsroom.fb.com/company-info/.
[7] https://www.statista.com/statistics/398136/us-facebook-user-age-groups/; https://newsroom.fb.com/company-info/.
[8] https://newsroom.fb.com/news/2007/05/facebook-unveils-platform-for-developers-of-social-applications/. This unveiling took place at Facebook's first almost annual F8 conference, intended for developers and entrepreneurs who build products and services around the Facebook website.
[9] *Id.*

28. As a purported social media leader, Facebook knows the critical importance of protecting users' Personal Information from unauthorized access. Facebook also knows the multitude of harms that foreseeably flow to individual users when information is stolen or misused by criminals.

29. To its users, Facebook promotes and provides assurances of privacy and the ability for users to control what information is transmitted to third parties. Facebook has explicitly told its users that their Personal Information would not be sold, transferred, or otherwise shared to any advertisement network, data broker, or other advertising or monetization-related third party without their expressed consent.

30. The opening line of Facebook's Statement of Rights and Responsibility is unambiguous in its recognition that Facebook users "own" their Personal Information and that users may rely on Facebook to protect that information from unwarranted disclosure:

> **1. Privacy**
> Your privacy is very important to us. We designed our Data Policy to make important disclosures about how you can use Facebook to share with others and how we collect and can use your content and information. We encourage you to read the Data Policy, and to use it to help you make informed decisions.
>
> **2. Sharing Your Content and Information**
> You own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings.[10]

31. Facebook's CEO Mark Zuckerberg has also publicly acknowledged the importance of privacy on its platform—stating that people engage and share on Facebook because "they know their privacy is going to be protected."[11]

---

[10] Terms of Service, Statement of Rights and Responsibilities, FACEBOOK, https://www.facebook.com/terms.php.

[11] Catherine Clifford, *Mark Zuckerberg 9 months ago: People share on Facebook because 'they know their privacy is going to be protected'*, CNBC (April 3, 2018), https://www.cnbc.com/2018/04/03/zuckerberg-on-facebook-and-privacy-before-cambridge-analytica-scandal.html.

32. A vital feature of Facebook is the appearance of control users have over their sensitive Personal Information. Facebook's privacy settings purport to offer users degrees of control over the dissemination of their Personal Information. Specifically, Facebook gives users the option to share, privately with only certain individuals, with all of their Facebook friends, with friends of friends, or with all Facebook users.[12] Users reasonably expect their Personal Information will be accessible only to the extent they authorize such access.

33. In 2010, Facebook released its Graph API (application programming interface), which is a developer, or app-level, interface touted as a revolution in large-scale data provision. The Graph API is the primary way to get data into and out of the Facebook platform. Graph API v.1.0, in effect from April 2010 to April 2015, converted Facebook users' Personal Information into quite literally "objects."[13]

34. Facebook's Graph API v.1.0 allowed third party app developers to access and store on third party servers, the following user data ("Personal Information"):[14]

Basic Info (default)
uid
name
first_name
last_name
link
username
gender
locale
age_range

Extended Profile Properties (xpP)	
User Data	Friends Data
user_about_me	friends_about_me
user_actions.books	friends_actions.books
user_actions.music	friends_actions.music
user_actions.news	friends_actions.news
user_actions.video	friends_actions.video
user_activities	friends_activities
user_birthday	friends_birthday
user_checkins	friends_checkins
user_education_history	friends_education_history
user_events	friends_events
user_friends	friends_games_activity
user_games_activity	friends_groups
user_groups	friends_hometown
user_hometown	friends_interests
user_interests	friends_likes
user_likes	friends_location
user_location	friends_notes
user_notes	friends_online_presence
user_online_presence	friends_photo_video_tags
user_photo_video_tags	friends_photos
user_photos	friends_questions
user_questions	friends_relationship_details
user_relationship_details	friends_relationships
user_relationships	friends_religion_politics
user_religion_politics	friends_status
user_status	friends_subscriptions
user_videos	friends_website
user_website	friends_work_history
user_work_history	

Extended Permissions (xP)
ads_management
ads_read
create_event
create_note
email
export_stream
manage_friendlists
manage_notifications
manage_pages
photo_upload
publish_actions
publish_checkins
publish_stream
read_friendlists
read_insights
read_mailbox
read_page_mailboxes
read_requests
read_stream
rsvp_event
share_item
sms
status_update
video_upload
xmpp_login

35. Facebook's Graph API v.1.0 allowed third party app developers to access and collect Personal Information from users through the friends data scrape feature, including photos and videos, without users' consent, and even where a user's profile was set to private.

36. According to former Facebook platform operations manager, Sandy Parakilas, "tens or maybe even hundreds of thousands of developers" may have sought friends permission data before such access was terminated in 2015.[15] Parakilas explained how outside app developers have been able to access Facebook users' Personal Information:

> It's important to remember that apps on Facebook, when you use them, they ask you for permission to access specific kinds of data, whether it's your name or your e-mail address or your friends list or photos or other information. And once you click "Allow" or tap "Allow," all that information passes from Facebook to the application developer. And the problem is that, once the data goes to the developer, there is no insight into what the developer is doing with the data, and there is no control by Facebook as to what they do. This has been a known problem since 2010.[16]

37. As information is shared by these billions of unique users, Facebook is provided with sophisticated, exceedingly detailed data profiles. Facebook, through Graph API, permitted developers to tap into this abundance of Personal Information without any meaningful oversight and without Facebook users' consent.

38. Facebook was aware of its lax approach to data protection because the majority of problems that have now come to the surface were meant to be features, not bugs. Facebook's business model rests on collecting these highly personal and highly revealing data points and selling to third parties, without vetting or following up, the ability to use this data about individuals to target ads to them.

---

[15] https://www.theguardian.com/news/2018/mar/20/facebook-data-cambridge-analytica-sandy-parakilas.

[16] https://www.cbsnews.com/news/sandy-parakilas-former-facebook-manager-warned-company-privacy-risks-in-2012/.

39. Facebook permitted third parties to improperly and illicitly harvest user data, purposely turning a blind eye while it continued to tout "trust," "privacy," and other pseudo-uplifting marketing speak to its Facebook users.[17]

40. A former Facebook platform operations manager had warned Facebook executives of this major risk of misuse of user data as early as 2011 but was discouraged from auditing third parties'' use of Facebook users' data. Regarding the recent headlines that Cambridge Analytica had illegally scraped Plaintiffs' and class members' data to improperly influence and otherwise disrupt the outcome of the 2016 Presidential election that former manager stated: "It's been painful watching . . . because I know they could have prevented it."[18]

B. Cambridge Analytica's Harvesting of Facebook Users' Personal Information

41. In 2013, Alexander Nix was the leader of the special elections division of the Strategic Communication Laboratories Group ("SCL Group"), a London-based public relations firm that describes its expertise as "psychological warfare" and "influence operations."[19] The same year, Mr. Nix met with Steven Bannon (former executive chairman of the "alt-right" news network Breitbart and former Trump advisor). They joined forces with Robert Mercer (U.S. hedge fund billionaire and Republican donor) in a scheme to use personality profiling to influence voting behavior.

[17] Oliva Solon, *'A grand illusion': seven days that shattered Facebook's facade*, THE GUARDIAN (March 24, 2018), https://www.theguardian.com/technology/2018/mar/24/cambridge-analytica-week-that-shattered-facebook-privacy.
[18] Paul Lewis, *'Utterly horrifying': ex-Facebook insider says covert data harvesting was* routine, THE GUARDIAN (March 20, 2018), https://www.theguardian.com/news/2018/mar/20/facebook-data-cambridge-analytica-sandy-parakilas.
[19] *See, e.g.*, Sharon Weinberger, *You Can't Handle the Truth,* SLATE (Sept. 19, 2005), http://www.slate.com/articles/news_and_politics/dispatches/2005/09/you_cant_handle_the_truth.html.

42. With Mr. Mercer's $15 million investment, Cambridge Analytica was born and their efforts to "bring big data and social media to an established military methodology—'information operations'—then turn it on the U.S. electorate" soon began.[20]

43. Christopher Wylie, former employee of Cambridge Analytica, was a data expert who oversaw the misconduct complained of herein.

44. In 2014, Cambridge Analytica set out to acquire the behavioral data of American citizens. Mr. Wylie found that Cambridge University Psychometrics Center researchers had developed a technique to map personality traits based on Facebook users' profiles. The approach, the Psychometrics Center researchers said, could reveal more about a person than their parents or romantic partners knew.

45. To its credit, Cambridge University Psychometrics Center declined to work with Cambridge Analytica.

46. Mr. Wylie then solicited Dr. Aleksandr Kogan, then a psychology professor at Cambridge University. Kogan agreed to work with Cambridge Analytica; to harvest Facebook data "so that it could be matched to personality traits and voter rolls."[21]

47. By June 2014, Cambridge Analytica had paid over $800,000 for Dr. Kogan to begin surreptitiously harvesting Facebook user's Personal Information and transmit it to them.

48. Dr. Kogan created a U.K. company called Global Science Research, Ltd. ("GSR") and through GSR, created a Facebook app called "ThisIsYourDigitalLife"[22] ("YDL app"). The YDL app consisted of a personality quiz hosted on Qualtric (an online survey platform) that required Facebook login credentials to complete.

---

[20] Carole Cadwalladr, *The Cambridge Analytica Files 'I made Steve Bannon's psychological warfare tool': meet the data war whistleblower*, THE GUARDIAN (March 18, 2018), https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump (last visited April 5, 2018).

[21] *Id.*

[22] Different sources have called the app "thisismydigitallife" or have spelled the YDL app with different spacing variations but for all intents and purposes, Plaintiffs are referring to the same app.

49. Posing as an academic researcher, Cambridge Analytica and Dr. Kogan utilized Amazon's Mechanical Turk ("MTurk") program to recruit participants to complete the personality quiz. Participants were offered $0.50-$2.00 to complete the quiz.

50. When participants responded to Kogan's request and expressed interest in completing the personality quiz, Kogan sent them a link to his Facebook application. Participants then completed the personality quiz, but to receive payment they were told that they needed to allow the quiz app access to their Facebook data for academic purposes. "And not just theirs, but their friends' too. On average, each 'seeder'—the people who had taken the personality test, around 320,000 in total—unwittingly gave access to at least 160 other people's profiles, none of whom would have known or had reason to suspect. What the email correspondence between Cambridge Analytica employees and Kogan shows is that Kogan had collected millions of profiles in a matter of weeks." [23] But no one "at Cambridge Analytica had checked that it was legal."[24]

51. At no time did Cambridge Analytica, Dr. Kogan, or GSR inform participants that their Personal Information was going to be used for non-academic purposes, including the intended improper use for electoral targeting.

52. At no time did Cambridge Analytica, Dr. Kogan, or GSR obtain permission from its YDL app users' Facebook friends to harvest their personal data.

53. Cambridge Analytica failed to inform or obtain permission because it knew it was not performing academic research. Instead, what it wanted and what it ultimately received, was access to the Personal Information of each YDL app user and *all* of that user's Facebook friends'

[23] Carole Cadwalladr, *The Cambridge Analytica Files 'I made Steve Bannon's psychological warfare tool': meet the data war whistleblower*, THE GUARDIAN (March 18, 2018), https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump (last visited April 5, 2018).

[24] Carole Cadwalladr, *The Cambridge Analytica Files 'I made Steve Bannon's psychological warfare tool': meet the data war whistleblower*, THE GUARDIAN (March 18, 2018), https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump (last visited April 5, 2018).

Personal Information. While the exact information that GSR provided to Cambridge Analytica is unknown, GSR had access to all Personal Information available through Graph API v.1.0 including the names, video, images, and photos of millions of Facebook users.[25]

54. The YDL app was so successful that from approximately 320,000 "seeders" who unwittingly completed the quiz, Defendant gained access to not only their Personal Information but also to over 87 million Facebook users' Personal Information.

55. The whistleblower, Mr. Wylie, confirms that there are receipts, invoices, emails, legal letters—records that showed how, between June and August 2014, Cambridge Analytica harvested the profiles of tens of millions of Facebook users.

56. The YDL app was used by Cambridge Analytica to create "psychographic" profiles which were then used to make predictions about people's behaviors and to create predictions about what people will do and what motivates them. This allowed Cambridge Analytica to design targeted political ads—using stolen Personal Information to play to unsuspecting users' preferences in efforts to influence their political views and choices.

C. Facebook Learns of YDL App's Data Collection and Fails to Act

57. Mr. Wylie confirms that Facebook should have known that the YDL app was collecting users' information at the time as its security protocols would have been triggered due to the enormous amount of data that the YDL app was pulling from Facebook's Graph API.

58. By the end of 2015, Facebook was notified that the data extracted by the YDL app had been transmitted to Cambridge Analytica. Instead of notifying its users, Facebook sat on this information for months taking no action. When Facebook finally took steps in mid-2016, Facebook's remedial action was limited.

[25] https://medium.com/tow-center/the-graph-api-key-points-in-the-facebook-and-cambridge-analytica-debacle-b69fe692d747.

59. Mr. Wylie, who responded to Facebook's request to delete the illicitly obtained data, was astonished by Facebook's lackluster response. Facebook made zero effort to get the data back and did nothing to confirm that the data was even deleted.

60. In the weeks leading up the 2016 presidential election, Mark Zuckerberg's trusted mentor and longtime investor, Roger McNamee, sounded the alarm about platform manipulation. Facebook executives brushed his concerns aside.[26]

61. To date, all data improperly obtained by Cambridge Analytica still has not been deleted.

62. This mass data collection was not only permitted, but also incentivized by Facebook, which sought to encourage developers to build on its platform, which upon information and belief, financially benefitted Facebook.

D. Facebook's Wrongdoing Finally Exposed

63. Facebook's inadequate data security practices and systematic failure to enforce its own ineffective data security policies were exploited for financial and political gain by third party app developers.

64. On March 17, 2018, Facebook's actions were finally made public.

65. *The Guardian* published an article, based on information obtained from Mr. Wylie, which detailed Cambridge's mining of over 87,000,000 Facebook users' Personal Information and its employment of that data to target individuals with its psychological operations to influence their views during the 2016 presidential election.[27]

66. After Facebook's wrongdoing was exposed, Facebook finally suspended Cambridge Analytica's and its affiliates' access to Facebook's platform.

[26] Lila MacLellan, *Maybe Mark Zuckerberg shouldn't have blown off his mentor*, QUARTZ AT WORK (March 20, 2018), https://work.qz.com/1233606/maybe-facebook-ceo-mark-zuckerberg-shouldnt-have-blown-off-his-mentor-roger-mcnamee/.
[27] *Id.*

67. Only in the aftermath of this news, Facebook has been attempting to salvage its brand and rebuild consumer trust by revamping its privacy policies.

68. Facebook's CEO Mark Zuckerberg publicly refused to appear before Parliament to answer questions regarding YDL. On the afternoon of April 4, 2018, after rebuffing Parliament, Facebook published a new data policy on its website. The new data policy is inadequate and so vague as that it continues to allow improper access to user data.

69. Facebook's stopgap measures fail to provide an adequate remedy or prevent further improper and illegal conduct. Personal Information already compromised remains dangerously vulnerable and open to further abuse. None of Facebook's measures constitute adequate notice to affected consumers. Further, Facebook has a history of failing to enforce its own data security policies.

E. Plaintiffs' Experience

70. Plaintiffs' Personal Information was shared with third parties, including Cambridge Analytica, without their knowledge or consent.

71. Plaintiffs and class members were harmed by third party app developers unlawfully obtaining their Personal Information.

72. Plaintiffs and class members have been injured in a number of ways, including: (i) they have lost control over their Personal Information and how it is used, as promised by Facebook; (ii) the value of their Personal Information, for which there is a well-established market, has diminished because it is no longer private; (iii) their Personal Information has been misused and is vulnerable to continued misuse; and (iv) they will have to spend time and money securing their Personal Information, protecting their identities, monitoring their accounts and credit and/or paying for further identity theft protection services in the wake of Cambridge Analytica's harvesting of Personal Information, to make sure their identities were not stolen and mitigating misuse of their Personal Information.

CLASS ACTION ALLEGATIONS

73. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

74. Plaintiffs bring this action on behalf of themselves and all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

75. Plaintiffs seek to represent the following Class:

Nationwide Class

All persons who registered for Facebook in the United States and whose Personal Information was obtained by third parties through Facebook's Graph API's "extended permissions" functionality.

76. Excluded from the Class are Facebook, its current employees, coconspirators, officers, directors, legal representatives, heirs, successors and wholly or partly owned subsidiaries or affiliated companies; the undersigned counsel for Plaintiffs and their employees; and the judge and court staff to whom this case is assigned. Plaintiffs reserve the right to amend the definition of the Class if discovery or further investigation reveals that the Class should be expanded or otherwise modified.

77. **Numerosity and Ascertainability:** Plaintiffs do not know the exact size of the Class or the identities of the Class Members since such information is the exclusive control of Facebook. Plaintiffs believe that the Class encompasses approximately over 87,000,000 individuals who are geographically dispersed throughout the United States. The number of members in the Class are so numerous that joinder of all Class Members is impracticable. The names, addresses, and phone numbers of class members are identifiable through documents maintained by Facebook.

78. **Commonality and Predominance:** The action involves common questions of law and fact, which predominate over any question solely affecting individual Class Members, including:

a. Whether Facebook gave Plaintiffs and class members effective notice of its program to collect their Personal Information;

b. Whether Facebook represented that Plaintiffs' and class members' Personal Information would be protected from disclosure absent their consent;

c. Whether Facebook owes any duty to Plaintiffs and class members with respect to maintaining, securing, or deleting their Personal Information;

d. To what degree Facebook has the right to use Personal Information pertaining to Plaintiffs and class members;

e. Whether Facebook owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, safeguarding, and/or obtaining their Personal Information;

f. Whether Facebook breached a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, safeguarding, and/or obtaining their Personal Information;

g. Whether the egregious breach of privacy and trust alleged in the Complaint was foreseeable by Facebook;

h. Whether Facebook intentionally exposed Plaintiffs' and class members' Personal Information to Cambridge Analytica;

i. Whether Facebook violated the Stored Communications Act;

j. Whether Facebook violated Plaintiffs' and class members' privacy rights;

k. Whether Facebook's conduct was an unlawful or unfair business practice under Cal. Bus. & Prof. Code § 17200, *et seq.*;

l. Whether Plaintiffs and the Class are entitled to equitable relief, including, but not limited to, injunctive relief and restitution/disgorgement; and

m. Whether Plaintiffs and the Class are entitled to actual, statutory, or other forms of damages, and other monetary relief.

79. Facebook engaged in a common course of conduct giving rise to the legal rights sought to be enforced by this action and similar or identical questions of statutory and common law, as well as similar or identical injuries, are involved. Individual questions, if any, pale in comparison to the numerous common questions that predominate this action.

80. **Typicality:** Plaintiffs' claims are typical of the other class members' claims because all class members were comparably injured through Facebook's substantially uniform misconduct as described above. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other class members, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and class members arise from the same operative facts and are based on the same legal theories.

81. **Adequacy:** Plaintiffs are adequate Class representatives because their interests do not conflict with the interests of the other members of the Classes they seek to represent; Plaintiffs have retained counsel competent and experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously. The Class' interest will be fairly and adequately protected by Plaintiffs and their counsel.

82. **Superiority**: A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and the other class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Facebook, so it would be virtually impossible for the members of the Classes to individually seek redress for Facebook's wrongful conduct. Even if class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

CLAIMS FOR RELIEF

COUNT ONE

Violations of the Stored Communications Act

18 U.S.C. § 2701, *et. seq.*

83. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

84. Plaintiffs, individually and on behalf of class members, assert violations of 18 U.S.C. §§ 2702(a) for Facebook's unlawful disclosure/divulging of the content of Plaintiffs' and class members' communications to third parties, including but not limited to SCL, Cambridge Analytica, Aleksandr Kogan, and GSR.

85. The Stored Communications Act ("SCA") prohibits a person from intentionally accessing without (or in excess of) authorization a facility through which an electronic communications service is provided and thereby obtaining an electronic communication while it is in "electronic storage." 18 U.S.C. § 2701(a).

86. The SCA defines "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and any storage of such communication by an electronic communication service for purposes of backup protection of such communication."

87. The servers Facebook uses to provide its electronic communications service to Facebook users are a "facility" within the meaning of the SCA.

88. Facebook is a "person" within the meaning of the SCA.

89. Facebook's provision of 'users' personal data with third parties as alleged herein exceeded any authorization from any party to the personal data at issue.

90. Because of the architecture of Facebook's servers, the sharing of personal data among Facebook users results in and constitutes interstate data transmissions.

91. The acquisition of Class Members' personal Facebook data—which constitute "communications" pursuant to the SCA—by Cambridge Analytica exceeded authorization to the personal data at issue.

92. Because of the architecture of Facebook's servers, the sharing of personal data among Facebook users results in and constitutes interstate data transmissions.

93. Pursuant to 18 U.S.C. § 2707(c), Plaintiffs and class members are entitled to minimum statutory damages of $1,000 per person, punitive damages, costs, and reasonable attorneys' fees.

COUNT TWO

Violations of the California's Right of Publicity Statute

Cal. Civil Code § 3344

94. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

95. California Civil Code § 3344 prohibits the use of a person's name, voice, signature, photograph, or likeness in connection the sale of goods or services without first obtaining that person's consent.

96. Defendant Facebook violated this section by allowing access to Plaintiffs' and class members' Personal Information—including names, photographs, and video—as a service to third parties. On information and belief, the use of images, photographs, and names of Plaintiffs and Class Members was integral to the services Facebook offered third party app developers such as Cambridge Analytica; third party app developers would not have purchased services from Facebook (including advertisements) without the Personal Information. Indeed, the value of the services Facebook offered to third party app developers was derived from the Personal Information.

97. Prior to using Plaintiffs' Personal Information, Facebook never obtained informed consent from Plaintiffs with respect to use by app developers of Plaintiffs' Personal Information.

98. Facebook and third party app developers profited from the commercial use of the Plaintiffs' likeness; yet, Plaintiffs did not receive any compensation in return for this use.

99. According to California Civil Code § 3344(a), Plaintiffs seek the greater of $750 per incident or the actual damages suffered, plus any profits attributable to Facebook's use of the unauthorized use not calculated in actual damages. Plaintiffs also reserve the right to seek punitive damages, costs, and reasonable attorney's fees as allowed under this statute.

COUNT THREE

Violations of the California Unfair Competition Law

Cal. Bus. & Prof. Code § 17200, *et. seq.*

100. Plaintiffs incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

101. Facebook's conduct as alleged herein constitutes unfair, unlawful, or fraudulent business acts or practices as proscribed by Section 17200, *et seq.*, of the California Business & Professions Code ("UCL").

102. Facebook's conduct also constitutes "unlawful" business acts or practices by virtue of Defendant's violation of the Stored Communications Act, 18 U.S.C. §§ 2701, et seq.; Cal. Civ. Code § 3344 and Cal. Pen. Code § 637.7.

103. Plaintiffs and class members reasonably relied on representations from Facebook that third parties could not access personal data absent their consent (including representations in Facebook's operative terms of service that omitted disclosure of the data that could be acquired, without consent, via the "extended permission" functionality). All of the above-described activity constitutes "fraudulent" business acts or practices. Plaintiffs and class members have an interest in controlling the disposition and dissemination of their private data, stemming from traditional privacy and autonomy rights.

104. Contrary to Plaintiffs' and class members' interests, each Defendant exercised control over the content of Plaintiffs' and class members' personal data, exploiting it for sale and

profit without consent. As a result, Facebook's conduct constitutes "unfair" business acts or practices.

105. Plaintiffs and class members have suffered injury in fact and lost money or property due to Facebook's business acts or practices. In particular, Plaintiffs' and class members' Personal Information was taken and it is in the possession of those who have used and will use it for their own advantage, including financial advantage, or was and is being sold for value, making it clear that the Personal Information has tangible value.

106. Plaintiffs and class members seek an order to enjoin Facebook from such unlawful, unfair, and fraudulent business acts or practices, and to restore to Plaintiffs and class members their interest in money or property that may have been acquired by Facebook by means of unfair competition.

COUNT FOUR

Invasion of Privacy by Intrusion

107. Plaintiffs incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

108. The California Constitution expressly provides for a right to privacy: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and *privacy*." Cal. Const., art. 1, § 1 (emphasis added).

109. California common law also recognizes the tort of invasion of privacy.

110. Facebook's terms of service provide that its users' Personal Information would not be released to third parties without permission and notice.

111. Plaintiffs and class members have an interest in preventing the unauthorized disclosure and/or misuse of their Personal Information and in conducting their personal activities

without intrusion or interference, including the right to not to have their Personal Information used by Cambridge Analytica and others for others' benefit.

112. Facebook intentionally intruded on Plaintiffs' and class members' private place, conversation, matter, seclusion, solitude and relationships and otherwise invaded their right to privacy without consent and permission.

113. Facebook's intrusive conduct was and is highly objectionable to reasonable persons and constitutes an egregious intrusion on Plaintiffs' and class members' rights to privacy and a breach of social norms underlying the privacy right.

114. As a direct and proximate result of Facebook's invasion of Plaintiffs' and Class Members' privacy, Plaintiffs and Class Members suffered injuries, damages, losses or harm, including but not limited to annoyance, interference, concern, lost time, the loss of personal property, and the need for the cost of effective credit and privacy security, justifying an award of compensatory and punitive damages.

COUNT FIVE

Unjust Enrichment

115. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

116. As a result of Defendant Facebook allowing third parties to access the Personal Information of Plaintiffs and class members, Facebook improperly obtained and misused the Personal Information of Plaintiffs and Class Members for its own benefit.

117. Facebook received millions of dollars in revenue from the sale and misuse of Plaintiffs' and class members' Personal Information.

118. This revenue was a benefit conferred upon Facebook by Plaintiffs and the Classes.

119. Facebook had knowledge of the monetary benefits conferred by Plaintiffs and class members.

120. Facebook was unjustly enriched by retaining the revenues obtained through falsehoods, deception, and breach of trust; Plaintiffs and each Class member are entitled to recover the amount by which Facebook was unjustly enriched at their expense.

121. Accordingly, Plaintiffs, on behalf of class members, seek damages against Facebook in the amounts by which Facebook has been unjustly enriched at Plaintiffs' and class members' expense, and such other relief as this Court deems just and proper.

RELIEF REQUESTED

122. Plaintiffs, individually and on behalf of class members, request that the Court enter judgment in their favor and against Facebook, as follows:

a. Certification of the proposed classes, including designation of Plaintiffs as class representatives and appointment of Plaintiffs' counsel as Class Counsel;

b. Judgment against Facebook for Plaintiffs' and class members' asserted causes of action;

c. Appropriate declaratory relief against Facebook;

d. Preliminary and permanent injunctive relief against Facebook;

e. An Order of disgorgement wrongfully obtained profits;

f. An award to Plaintiffs and class members of actual, statutory, and punitive damages as permitted by applicable laws;

g. An award of attorneys' fees and other litigation costs reasonably incurred; and

h. Any and all relief to which Plaintiffs and the Class may be entitled or such other relief that the Court deems appropriate.

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and all others similarly situated, hereby demand a trial by jury on all the issues so triable.

DATE: September 18, 2018

BLEICHMAR FONTI & AULD LLP

By: */s/ Lesley E. Weaver*
Lesley E. Weaver

Lesley E. Weaver (SBN 191305)
Matthew S. Weiler (SBN 236052)
Emily C. Aldridge (SBN 299236)
555 12th Street, Suite 1600
Oakland, CA 94607
Tel.: (415) 445-4003
Fax: (415) 445-4020
lweaver@bfalaw.com
mweiler@bfalaw.com
ealdridge@bfalaw.com

Plaintiffs' Counsel

KELLER ROHRBACK L.L.P.

By: */s/ Derek W. Loeser*
Derek W. Loeser

Derek Loeser (admitted *pro hac vice*)
Lynn Lincoln Sarko (admitted *pro hac vice*)
Gretchen Freeman Cappio (admitted *pro hac vice*)
Cari Campen Laufenberg (admitted *pro hac vice*)
1201 Third Avenue, Suite 3200
Seattle, WA 98101
Tel.: (206) 623-1900
Fax: (206) 623-3384
dloeser@kellerrohrback.com
lsarko@kellerrohrback.com
gcappio@kellerrohrback.com
claufenberg@kellerrohrback.com

Christopher Springer (SBN 291180)
801 Garden Street, Suite 301
Santa Barbara, CA 93101
Tel.: (805) 456-1496
Fax: (805) 456-1497
cspringer@kellerrohrback.com

Plaintiffs' Counsel